North Dakota
Homeland Security
Anti-Terrorism Summary

The North Dakota Open Source Anti-Terrorism Summary is a product of the North Dakota State and Local Intelligence Center (NDSLIC). It provides open source news articles and information on terrorism, crime, and potential destructive or damaging acts of nature or unintentional acts. Articles are placed in the Anti-Terrorism Summary to provide situational awareness for local law enforcement, first responders, government officials, and private/public infrastructure owners.

NDSLIC Disclaimer

Quick Links

North Dakota

North Dakota's second case of West Nile virus this year confirmed. Bismarck, North Dakota, has a second confirmed human case of West Nile virus. The state health department said today that the Ward County boy was not hospitalized. West Nile virus was first identified in North Dakota in 2002. Since then, nearly 1,300 human cases of the mosquito-borne illness have been reported. Last year, there was only one confirmed case in the state. The highest human case total in North Dakota was 617, seven years ago. Source: http://www.grandforksherald.com/event/article/id/170090/group/homepage/

Thousands hit by CableOne phone, Internet outage. CableOne of Fargo, North Dakota said phone and Internet service in the area was disrupted after a botched equipment update the week of July 19, causing two days of outages affecting thousands of users. New equipment is being sent, and crews had hoped to repair service by July 24 in most instances, the general manager said. The installation of a new computer that is essentially a giant router connecting homes to the wider Internet created the connection failures. The upgrade gone awry was meant to increase the speed of Internet access. Phone service was also affected because it is Internet based. Source: http://www.inforum.com/event/article/id/285837/

Insecticide spill closes part of I-94; no injuries reported. A hazardous materials spill on Interstate 94 in North Dakota caused no injuries but detoured traffic for about 7 hours July 23. The incident began about 9:30 a.m. when a farm truck spilled canisters, which broke open by mile marker 232 near Cleveland. The canisters contained several gallons of an insecticide marketed as Govern as well as an emulsifier marketed as Trophy Gold. It was unknown how much spilled, but up to 20 gallons of insecticide, and 30 gallons of the emulsifier were on the truck. The Material Safety Data Sheet for Govern indicates fumes from the substance are an inhalation hazard and irritant, and the chemical is flammable. The eastbound lanes of Interstate 94 were closed between Jamestown and Medina for several hours, with traffic rerouted onto state highways 30 and 46 and U.S. Highway 281. The materials were cleared from both lanes to allow limited traffic to pass the site by 4:30 p.m. The North Dakota Department of Transportation used dirt to cover the insecticide and absorb the chemical. Source: http://www.inforum.com/event/article/id/285840/

Regional

(Minnesota) **Traffic moves as lift bridge brought back down.** Traffic is moving on and off Park Point again now that Duluth, Minnesota crews have returned the Aerial Lift Bridge to its lowered position. The bridge was stuck in the lifted position for more than two hours after an apparent lightning strike. "A lightning strike took out traffic lights," said the Aerial Lift Bridge supervisor. "They are in our circuitry to allow the bridge to work." The bridge was up for a vessel to pass through when the outage occurred about 5:30 p.m., he said. Bridge staff brought the bridge down manually while

drivers waited for two hours or more to cross. Source: http://www.duluthnewstribune.com/event/article/id/174797/

(Minnesota) **Drill scheduled to test Prairie Island nuclear plant.** Several public agencies will participate in a drill July 27 to test the response to an emergency at the Prairie Island nuclear plant in Red Wing, Minnesota. Citizens in the area are being alerted to expect seeing emergency responders carrying out their duties during the exercise. Activities near the plant will take place in Dakota and Goodhue counties in Minnesota and Pierce County in Wisconsin. Participants will include the Minnesota Department of Public Safety Division of Homeland Security and Emergency Management; Xcel Energy, which operates the plant; the Prairie Island Indian community; other Minnesota agencies, including the Departments of Agriculture, Health, Human Services and Transportation; officials of Dakota, Goodhue and Pierce counties; and the federal Department of Homeland Security. Source: http://www.startribune.com/local/99238739.html?elr=KArksi8cyaiUjc7YUiD3aPc:_Yyc:aU7DYaGEP7vDEh7P:DiUs

(Montana) **Cardinal Creek fire grows to 1200 acres.** The Flathead National Forest in Montana is managing the Cardinal Creek Wildland Fire in the Bob Marshall Wilderness, approximately 18 miles southeast of Condon, Montana. The fire was reported July 25. Aerial monitoring conducted the evening of July 26 indicates the fire is approximately 1,200 acres. The fire is actively burning on the west and north sides of Kid Mountain above Gordon Creek, and in the drainage divide between Gordon Creek and Youngs Creek on the Spotted Bear Ranger District. The Flathead National Forest is managing the fire for multiple objectives, including public and firefighter safety, allowing the natural role of fire in wilderness and protecting values at risk. The fire is burning in heavy timber, with a large component of down and dead fuels. Smoke is visible from the Seeley Lake area in the Swan Valley, and from Augusta and Choteau along the eastern side of the continental divide. Recent lightning in the area is suspected to be the cause of the fire. Source: http://www.nbcmontana.com/keci/24403315/detail.html

(Montana) **Bitterroot fire grows to 100+ acres.** Some 80 firefighters July 26 will begin helping crews battling a wildfire near Hamilton, Montana that continues to burn. The Bitterroot National Forest Service reports that nearly 100 acres have been consumed in the Dominic Point area. The fire is located 12 miles northeast of Hamilton, just 2 miles west of Willow Mountain Lookout. There are 20 firefighters and four engines battling it, along with four helicopters which are performing water drops. Four planes are also assisting in the efforts. Bitterroot National Forest officials said all of their available crews are fighting the blaze. The cause of the fire is unknown at this time, but it may be a holdover fire which was sparked by last week's lightning storm. Source: http://www.krtv.com/news/bitterroot-fire-grows-to-100-acres/

National

(Virginia) **Bad-tasting drinks lead to felonies.** A 29-year-old Fredericksburg, Virginia man poured a bleach-based cleaner into his co-workers' drinks, police said. A Spotsylvania sheriff's spokesman said the incident occurred about 8:30 a.m. July 26 at Denny's Restaurant in the 5300 block of Jefferson Davis Highway. Two employees reported their drinks tasted like they had been tainted with bleach. The employees, a man and a woman, had left their coffee and soda at the waiter/waitress station and

had taken sips at different times. They told the manager and mentioned another employee who they believed might have been responsible. The manager called the sheriff's office, and the deputy talked with the suspect. The suspect first claimed that he must have accidentally gotten the cleaner into the drinks while he was cleaning the waiter/waitress station. The suspect later admitted that he never cleans that area. The substance put in the drinks, Eco San, is a bleach-based liquid sanitizer. The suspect was charged with two counts of altering a drink with the intent to harm, and he was placed in the Rappahannock Regional Jail under no bond. The Class 3 felonies each carry maximum prison sentences of 20 years. Source: http://fredericksburg.com/News/FLS/2010/072010/07282010/564499

(Michigan) **Wildlife soaked in oil, odor spreads after pipeline leaks 840K gallons into Kalamazoo River.** Officials say 840,000 gallons of oil has leaked from a pipeline into a creek that flows into the Kalamazoo River in southwest Michigan, threatening wildlife and introducing a pungent odor to the area. The general manager for Enbridge Liquids Pipelines says a malfunction caused the leak in the 30-inch pipeline July 26. Houston-based Enbridge and the Calhoun County Sheriff's Office of Emergency Management say the pipeline pumps were shut down as soon as the leak was discovered. The pipeline carries about 8 million gallons of oil a day from Griffith, Indiana to Sarnia, Ontario. The oil spilled into Talmadge Creek, which flows northwest into the Kalamazoo River. Source: http://www.latimes.com/business/nationworld/wire/sns-ap-us-michigan-river-oil-spill,0,1712391.story

(Louisiana) **Deepwater Horizon alarm had been 'inhibited,' technician testifies.** An alarm system on the Deepwater Horizon had been "inhibited" for about a year before the April 20 explosion that killed 11 workers and started the worst oil disaster in the nation's history, the platform's chief electronics technician testified to a federal panel July 23. An inhibited mode means sensors for toxic or combustible gases or fire are active and will alert the platform's computer system, but the computer does not trigger an audible or visual alarm, a technician told the six-member panel. Supervisors on the Transocean rig were aware that the alarm system had been inhibited. "When I discovered about a year ago it was inhibited, I inquired as to why it was inhibited, and the explanation I got is that ... they did not want people woke up at 3 o'clock in the morning due to false alarms," the technician said. The rig's general alarm system also has normal and override settings, the technician testified. Under an override setting, the computer will not recognize the sensor information for any purpose, he said. The alarm system's visual alerts were on light towers throughout the rig, he said. A red light signified fire, a yellow light meant toxic gas, and a blue light indicated combustible gases. Published reports have indicated that investigators are looking into whether a rapidly expanding methane gas bubble escaped from the well 5,000 feet below the surface, busting through seals and barriers before shooting up the drill column and exploding. Source: http://www.cnn.com/2010/US/07/23/gulf.platform.alert/index.html?hpt=T1

INTERNATIONAL

Death toll tops 300 in Pakistan flooding. The death toll for three days of flooding in Pakistan rose to 313 Friday as rains swelled rivers, inundated villages and triggered landslides, officials said. The toll was expected to increase because many people were reported missing, Pakistan's English newspaper Dawn reported. A spokesperson of the private non-profit Edhi Foundation said at least 291 people died in parts of Khyber Pakhtunkhwa province during the past few days. Part of a recently constructed dam in the province's Charsadda district collapsed, submerging a reported 5,000 homes

and stranding up to 400,000 people, officials said. “A rescue operation using helicopters cannot be conducted due to the bad weather, while there are only 48 rescue boats available for rescue,” the province’s information said Thursday. The highway linking Peshawar to Islamabad was closed after water washed away bridges, the government said. Although northwestern Pakistan bore the brunt of the flooding, Dawn said the southwestern province of Balochistan also was hit by the rains and crops in Punjab province were ruined. Source: http://www.upi.com/Top_News/International/2010/07/30/Death-toll-tops-300-in-Pakistan-flooding/UPI-60931280489063/

Russia foils passenger plane hijacking. Russian special forces quickly overpowered a man after he briefly seized a plane with 105 passengers and crew at a Moscow airport July 29, officials said. The plane, which departed from the southern Russian city of Mineralniye Vody, was landing at Moscow’s Domodedovo Airport when a 30-year-old passenger handed a note to a crew member demanding a meeting with the Russian prime minister, according to a statement by federal investigators. The plane was freed two hours later by special forces who boarded the plane disguised as doctors after the hijacker agreed to allow several passengers to receive medical attention. It was unclear how he had gained control of the plane. Russian news agencies cited police officials as saying the man was not armed. Mineralniye Vody is in Russia’s troubled North Caucasus region, which suffers daily violence attributed to separatist militants. Source: http://www.cbsnews.com/stories/2010/07/29/ap/world/main6724942.shtml

New flood surge hits China’s Three Gorges Dam. Vast amounts of water have been released from behind China’s Three Gorges Dam in recent days. The dam faced a second test as floods pushed the water in its reservoir to near its capacity, state media said. Heavy rain on the Yangtze River created a surge that neared last week’s record. China’s worst flooding in a decade has killed at least 823 people and left 437 missing, authorities said. In the latest developments, 21 people are feared dead in a landslide, while 37 people are known to have died after a bridge collapsed. Engineers at the Three Gorges Dam said the reservoir water level rose to 518 feet (158 meters) at 8 a.m. local time July 28, the state-run Xinhua news agency said. The maximum capacity is 175 meters. Authorities have warned communities downstream to prepare for rising water levels as the dam’s huge spill gates release torrents of water. The flow into the dam’s reservoir, however, is lower than last week’s peak of 70,000 cubic meters per second. Source: http://www.bbc.co.uk/news/world-asia-pacific-10784666

Freak wave damages Japan supertanker off Oman. A Japanese oil tanker was damaged by unknown reasons in the Strait of Hormuz. The ship’s owners reported an explosion on board and said it may have been caused by an attack, but a port official who spoke to the crew said there was no evidence of an attack. No oil leaked from the supertanker, named M Star, although some members of the 31-strong crew were injured, said a general manager at the UAE port of Fujairah where the ship was due to arrive at 5 p.m. July 28 “The cause of the incident was a freak wave and there is damage in the upper accommodation decks of the ship and a few injured people on board,” he told Reuters. “The ship is not being tugged and there is no damage to the engine.” Oman’s coast guard cited “a tremor” as the cause of the incident, while an official from the Omani transport ministry said it was “business as usual” in the Strait of Hormuz. A seismologist in nearby Iran said an earthquake with a magnitude of about 3.4 happened in Bandar Abbas. “A crew member saw light on the horizon just before the explosion, so the captain believes there is a possibility it was caused by an outside attack.” Source: http://www.reuters.com/article/idUSTRE66R1ZX20100728

Banking and Finance Industry

Cheat an ATM? Spy on secure web traffic? Hackers show how. Researchers have uncovered new ways that criminals can spy on Internet users even if they are using secure connections to banks, online retailers or other sensitive Web sites, as determined hackers can sniff around the edges of encrypted Internet traffic to pick up clues about what their targets are up to. The problem lies in the way Web browsers handle Secure Sockets Layer, or SSL, encryption technology, according to the researchers. Encryption forms a kind of tunnel between a browser and a website's servers, scrambling data so it is indecipherable to prying eyes. SSL is widely used on sites trafficking in sensitive information, such as credit card numbers, and its presence is shown as a padlock in the browser's address bar. The approach by the researches was not to break it. They wanted to see instead what they could learn from what are essentially the breadcrumbs from people's secure Internet surfing that browsers leave behind and that skilled hackers can follow. Their attacks would yield all sorts of information. It could be relatively minor, such as browser settings or the number of Web pages visited. It could be quite substantial, including whether someone is vulnerable to having the "cookies" that store usernames and passwords misappropriated by hackers to log into secure sites. Source: http://www.foxnews.com/scitech/2010/07/30/web-security-fears-black-hat/?test=latestnews

Black Hat conference demonstration reveals ATM security risk. At the Black Hat conference in Las Vegas, IOActive's director of security research gave a demonstration of how he learned to crack the security of various stand alone ATMs after coming across several errors and security weaknesses in their [software] coding, allowing him to gain full access to the machines' safes. He wrote multiple programs to exploit some of the machines' weaknesses including one that allows him to gain remote entry without the need of a password, which he calls Dillinger, and a second program, Scrooge, that relies on a back-door entry with the ability to conceal itself from the machine's main operating system. In the case of Triton's ATMs, the researcher found the motherboard of the machine was sorely lacking in physical security, and once he had gained access to it, he was easily able to use a similar back-door technique then simply trick the machine into thinking that the hack was actually a legitimate update. So far, the researcher has attempted to hack four different ATMs and, as he demonstrated at the conference, he has found that the same "game over vulnerability" has enabled him to crack every one of them. Source: http://www.daniweb.com/news/story300369.html

Russian gang uses botnets to automate check counterfeiting. The director of malware research for Atlanta-based SecureWorks has uncovered a sophisticated check-counterfeiting ring that uses compromised computers to steal and print millions of dollars worth of bogus invoices, and then recruit money mules to cash them. The highly automated scheme starts by infiltrating online check archiving and verification services that store huge numbers of previously cashed checks. It then scrapes online job sites for e-mail addresses of people looking for work and sends personalized messages offering jobs performing financial transactions for an international company. The scammers then use stolen credit-card data to ship near exact replicas of checks to those who respond. The director was able to track the operation by infecting a lab computer and observing its interactions with command and control channels. A database file the criminals carelessly exposed showed 3,285 checks had been printed since June of 2009 and 2,884 job seekers had responded to the employment offer. Assuming each check was written in amounts of $2,800, a threshold sum that brings increased

scrutiny to transactions, the director estimates the checks were valued at about $9 million. Source: http://www.theregister.co.uk/2010/07/28/automated_check_counterfeiting/

(New York) **Man armed with fake bomb robs West Babylon bank.** A man wearing what appeared to be an explosive device strapped to his body walked into a Chase Bank branch in West Babylon, New York early July 26 and demanded cash. The robber was given cash and fled through the back door. He was last seen on foot headed east toward Hubbards Path. The suspect was described as a white man between 50 and 60 years old, 5 feet 10 inches to 6 feet tall with a thin to medium build. He was clean-shaven with short, graying hair. He was wearing a pinstriped suit jacket, which was recovered at the scene. The robber discarded the device behind the shopping center where the bank is located. Emergency Service Section officers responded and determined the device was not a real bomb. Source: http://www.longislandpress.com/2010/07/26/man-armed-with-fake-bomb-robs-west-babylon-bank/

Citi, Apple disclose iPhone app security flaw. Banking giant Citigroup and iPhone maker Apple are encouraging users who downloaded Citi's banking application for the smartphone to upgrade to a new version after a security flaw was discovered in the application. The flaw accidentally saves personal information, including access codes, bill payment information and even bank account numbers, onto the iPhone or any computer it has been synchronized with. The Wall Street Journal reported approximately 117,600 customers has been affected by the flaw since the app was launched in Apple's App Store in March 2009, although the paper's unnamed source said no personal data was exposed. The paper also interviewed the CEO of mobile security specialist Lookout who warned that hackers could exploit flaws in banking applications in order to retrieve, and then exploit, personal information downloaded by the app. Many consumers, who may download multiple apps casually, may not be aware to what level of risk they are exposed, he said. Source: http://www.eweek.com/c/a/Midmarket/Citi-Apple-Disclose-iPhone-App-Security-Flaw-440879/

FDIC: Top 5 fraud threats. The chief of the Federal Deposit Insurance Corporation's Cyber Fraud and Financial Crimes Section recently released his top five list of fraud threats of concern to the FDIC: 1. Malware and Botnets; 2. Phishing; 3. Data Breaches; 4. Counterfeit Checks; 5. Mortgage Fraud. Malware and Botnets are software agents or robots that take over a user's computer are often the root causes of commercial payments fraud, i.e. corporate account takeover. Phishing has evolved from badly-written, bogus e-mails to well-crafted assaults via e-mail, telephone and text message. While most data breaches have occurred on the merchant and payments processor sides of the business, financial institutions are still deeply impacted by these losses. Although circulation of fake checks continues to drop, counterfeit check fraud remains prevalent. Mortgage fraud crimes committed against financial institutions, as well as mortgage rescue scams that affect consumers and mortgage holders, continue to plague the financial market. Source: http://www.bankinfosecurity.com/articles.php?art_id=2774

Seven banks closed on July 23. Federal and state banking regulators closed seven banks July 23, raising the number of failed institutions to 113 so far in 2010. The latest closings follow. SouthwestUSA Bank, Las Vegas was closed by the Nevada Financial Institutions Division, and the Federal Deposit Insurance Corporation (FDIC) was appointed receiver. The FDIC arranged for Plaza Bank, Irvine, California to buy the deposits of the failed bank. The estimated cost to the FDIC's Deposit Insurance Fund (DIF) will be $74.1 million. Sterling Bank, Lantana, Florida was closed by the

Florida Office of Financial Regulation, which appointed the FDIC as receiver. The FDIC arranged for IBERIABANK, Lafayette, Louisiana to buy the deposits of the failed bank. The estimated cost to the DIF will be $45.5 million. Crescent Bank and Trust Company, Jasper, Georgia was closed by the Georgia Department of Banking & Finance, which appointed the FDIC as receiver. The FDIC arranged for Renasant Bank, Tupelo, Mississippi to buy the deposits of the failed bank. The estimated cost to the DIF will be $242.4 million. Home Valley Bank, Cave Junction, Oregon was closed by the Oregon Department of Consumer and Business Services, which appointed the FDIC as receiver. The FDIC arranged for South Valley Bank & Trust, Klamath Falls, Oregon, to buy the failed bank. The estimated cost to the DIF is $37.1 million. Thunder Bank, Sylvan Grove, Kansas was closed by the Kansas Office of the State Bank Commissioner, which appointed the FDIC as receiver. The FDIC arranged for The Bennington State Bank, Salinas Kansas to buy the failed bank. The estimated cost to the DIF will be $4.5 million. Williamsburg First National Bank, Kingstree, South Carolina was closed by the Office of the Comptroller of the Currency, which appointed the FDIC as receiver. The FDIC arranged fro First Citizens Bank and Trust Company, Inc. Columbia, South Carolina to buy the failed bank. The estimated cost to the DIF is $8.8 million. Community Security Bank, New Prague, Minnesota was closed by the Minnesota Department of Commerce, which appointed the FDIC as receiver. The FDIC arranged for Roundbank, Waseca, Minnesota to buy the failed bank. The estimated cost to the DIF will be $18.6 million. Source: http://www.bankinfosecurity.com/articles.php?art_id=2780

Chemical and Hazardous Materials Sector

NRC amends regulations on export and import of nuclear equipment and material. The Nuclear Regulatory Commission (NRC) is amending its regulations to improve the agency's regulatory framework for the export and import of nuclear equipment, material and radioactive waste. In addition to making clarifications, updates and corrections to several provisions, the rule allows imports of sources under a general license, and revises the definition of radioactive waste for the purposes of export and import. The amendments, in a final rule published July 28 in the Federal Register, remove the requirements for licensees to obtain a specific license before importing Category 1 and Category 2 quantities of radioactive materials listed in Appendix P to 10 CFR 110. NRC or Agreement State licensees must be authorized to possess these sources domestically in order to import them under a general license. Importers are still required to provide notification of the import prior to shipment. (Thirty-seven states have agreements with the NRC under which the states license and regulate radioactive material.) The NRC is making this change because of enhancements made to the domestic materials licensing and regulatory framework since the terrorist attacks of September 11, 2001. Those security enhancements include background investigations, fingerprint checks and trustworthiness and reliability checks of personnel allowed unescorted access to risk-significant materials, physical intrusion barriers, coordination with local law enforcement, and enhanced security measures during transport. Source: http://www.nrc.gov/reading-rm/doc-collections/news/2010/10-133.html

NRC informs Areva of safety issues with EPR reactor design's computer systems. Nuclear Regulatory Commission staffers have informed AREVA NP that the company has yet to demonstrate how some aspects of the EPR reactor's digital instrumentation and control system meet NRC requirements. While the NRC's letter to AREVA acknowledges progress in resolving the issues, particularly the discussion during a June 25 public meeting and AREVA's July 1 letter proposing revisions to the

system, the NRC staff notes that additional information is necessary to determine the system's acceptability. Specifically, AREVA needs to better demonstrate that each safety division in the system can perform its function without relying on information originating from outside the safety division and is protected from adverse influence from outside the division. AREVA also needs to better demonstrate that data exchanged between safety and non-safety divisions are processed in a manner that does not adversely affect the function of the safety division. The staff continues its work on the remainder of the EPR design-certification application. The impact on the overall EPR certification-review schedule will be established after AREVA provides more details on its plans to revise the reactor's digital instrumentation and control system. Source: http://www.nrc.gov/reading-rm/doc-collections/news/2010/10-130.html

Rush and Waxman release Toxic Chemicals Safety Act. On July 22, the chair of a House subcommittee, and the chair of the House Committee on Energy and Commerce introduced H.R. 5820, the Toxic Chemicals Safety Act of 2010. "The introduction of this legislation marks a major step forward in our efforts to bring to current industry standards an important statute that, once it becomes law, will permanently shine the bright light of public disclosure on a range of chemicals that consumers encounter in a diverse array of products they use each and every day," said the chair of the House Energy and Commerce Subcommittee on Commerce, Trade, and Consumer Protection, which has slated a July 29 hearing on the bill. The legislation would amend the Toxic Substances Control Act of 1976 to ensure that the public and the environment are protected from risks resulting from chemical exposure. Source: http://eponline.com/articles/2010/07/23/rush-and-waxman-release-toxic-chemicals-safety-act.aspx

COMMERCIAL FACILITIES

(Massachusetts) **Explosive device found in front of Dollar Tree store.** An explosive device was found July 28 in front of a Dollar Tree store in the Home Depot Plaza on Revere Beach Parkway in Chelsea, Massachusetts, after a bomb squad responded to a report of a suspicious package. Officers determined that the package was some type of makeshift explosive. There was a fuse on the device but no mechanism for detonating it remotely. Police said that someone made a definite attempt to make and place the item. The bomb squad from the Boston Police Department assisted and removed the item. It was taken away and destroyed. Police said that they are following some leads, but there have been no arrests. Source: http://www.myfoxboston.com/dpp/news/local/explosive-device-found-in-front-of-dollar-tree-store-20100728

(Indiana) **Investigators: Device that prompted bomb scare fake.** Several people July 28 were evacuated from Bradford Place Collegiate Residences in Bloomington, Indiana, after a maintenance worker discovered a device that appeared to be a pipe bomb. Investigators said that the device that had been left in an apartment closet was fake. Bloomington police said a maintenance worker went into an apartment closet after a tenant had moved out and found two pipes tied together with a wire coming out of it. Police, firefighters and a bomb squad from Crane Naval Surface Warfare Center were called to the scene. A robot was sent in to retrieve the device, which investigators determined was not a bomb. Investigators believe it had been left there intentionally. Source: http://www.theindychannel.com/news/24423677/detail.html

(Florida) **Bomb threat closes Murdock shopping center in Charlotte County.** A three-hour bomb scare that shut down a Murdock, Florida shopping center July 27 has ended and authorities are now searching for two men last seen near the SUV that had a note saying a bomb was inside the vehicle. Investigators said the incident started when a 22-year-old Port Charlotte woman drove to the plaza with her young children to buy groceries at Save-a-Lot around 6 p.m. The woman parked and a dark truck with two white "scruffy-looking" men pulled alongside her Jeep SUV, and she could not get out. They exchanged glances, and the woman drove forward to find another parking space. She got out with her kids and went shopping. About 20 minutes later, she came out and noticed a note on her windshield that implied that the woman's car would explode if she started her vehicle. Deputies and firefighters evacuated the entire shopping center. The bomb squad arrived at 8:25 p.m. and deployed its robot along with two men in safety gear. The Charlotte County Sheriff's Office and Southwest Regional Bomb Squad gave the all-clear at 9:30 p.m. after evacuating all stores and traffic in Village Market Place on Tamiami Trail. Sheriff's detectives are analyzing the handwritten note for fingerprints. Source: http://www.heraldtribune.com/article/20100728/ARTICLE/307289997/2055/NEWS?Title=Bomb-threat-closes-Charlotte-County-shopping-center-&tc=ar

(California) **Explosive device disarmed near OC park.** An explosive device capable of causing "substantial damage" was found today near Yorba Regional Park in Los Angeles, California, prompting authorities to evacuate about a dozen homes and shut down La Palma Avenue for several hours. Someone put a substantial amount of explosive powder in a five-gallon water jug, sealed it off with tape and put a fuse in it. The fuse was lit at some point, but it did not detonate. The device had been there for hours before someone called police. The Orange County bomb squad detonated a portion of the device without setting off the powder so they could render the explosive inert. Investigators suspect it was the work of one or more pranksters. Source: http://www.myfoxla.com/dpp/news/local/explosive-device-orange-county-park-20100726

(Colorado; Utah) **Utah man arrested in sheepskin store fire.** A man who has been arrested on suspicion of starting a fire that destroyed a sheepskin store near Denver has been linked to two other fires in Utah, which destroyed business he allegedly deemed were cruel to animals, police said. He was arrested July 22. Federal prosecutors have charged the 34-year-old with one count of arson in connection with the fire at the Sheepskin Factory in Glendale, Colorado in April. He has not been charged in the other fires. The susepct allegedly told a friend that he started the fire that destroyed the Leather Factory in Salt Lake City in June and the Tiburon Restaurant in Sandy, Utah, which served foie gras. A Bureau of Alcohol, Tobacco, Firearms and Explosives agent said he called a friend that he had not seen in 12 years and referred to a Web site associated with the Animal Liberation Front. A posting on the Web site claimed responsibility for the fire in Glendale, saying it was done "in defense and retaliation for all the innocent animals that have died cruelly at the hands of human oppressors." The posting also claimed responsibility for the fires in Salt Lake City and contained the warning: "Be warned that making a living from the use and abuse of animals will not be tolerated." The FBI does not take such threats lightly. "Terrorism in the name of animal rights is every bit as dangerous and destructive as the other threats facing our country today," said a Denver FBI special agent in a statement. "The actions of [the suspect] resulted in significant property damage and worse, could have resulted in the loss of life." Source: http://www.forbes.com/feeds/ap/2010/07/23/general-us-sheepskin-factory-fire_7794200.html?boxes=Homepagebusinessnews

(Washington) **Homemade explosive found in portable toilet in Lakewood.** Police evacuated a small apartment complex and several businesses in Lakewood, Washington, after a device resembling a pipe bomb was found in a portable toilet July 23. About 60 people had been evacuated from the nearby apartment complex and businesses. A United Fite Services worker discovered the explosive around 9:15 a.m. while cleaning a SaniCan on Tacoma Public Utilities property next to a substation. The fuse had been lit but had not gone off. The worker alerted police, then notified Tacoma Power, a subsidiary of Tacoma Public Utilities. A Pierce County Sheriff's Office bomb squad defused the device and removed it from the Sanican. The Lakewood Police Department assistant chief said the device was not a pipe bomb but a homemade explosive made from several items, including a roman candle. Had it gone off, the explosive would have damaged the Sanican and injured anyone in it. Source: http://www.king5.com/news/local/Pipe-bomb-found-in-trash-bin-prompts-evacuations-in-Lakewood-99115149.html

(Oregon) **Pipe could have taken out Woodburn Inn.** A possible pipe bomb was discovered July 24 inside a Woodburn Inn motel room in Woodburn, Oregon. Police said the owner of the bomb is a man already in local jail on a warrant out of New Hampshire. Authorities said police learned the suspect had a warrant for his arrest out of New Hampshire "for a threat of [a] bomb" after pulling him over on "a routine traffic stop." The pipe did not contain explosives when it was found. However, it was blown up by state police as a precaution. The investigation closed Oregon state highway 99 East in Woodburn until just after 3 p.m. Oregon State Police bomb technicians responded to the scene. Six houses on Williams Street behind the Woodburn Inn were evacuated, in addition to about 15 businesses in the surrounding area. Source: http://www.katu.com/news/local/99174224.html

(Michigan) **McD's evacuated after bomb threat.** Employees at a Belding, Michigan McDonalds were evacuated from the restaurant early July 25 after receiving a bomb threat. Around 8:30 a.m. the McDonalds at 1125 W. State St. received a call from a person saying there was a bomb in the bathroom. The caller said if the employees did not bring money to him at the front door, he would come into the restaurant and blow it up. The Belding Police Department and Ionia County Sheriff Department searched the restaurant, but found no evidence of a bomb in the area. The scene was cleared around 11 a.m. Authorities said this incident is similar to a bomb threat that was called in July 21 at a Wal-Mart in Comstock Park. In that instance, a man called the business, stating a bomb was in one of the store's bathrooms. The Alpine Township fire chief stated the caller may have made some kind of demand for money as well. Source: http://www.woodtv.com/dpp/news/local/central_mich/McD's-evacuated-after-bomb-threat

Communications Sector

FCC, FDA Partner To Advance Telehealth. The Federal Communications Commission (FCC) and the U.S. Food and Drug Administration (FDA) have joined forces to help advance innovation and investment in wireless-enabled telehealth devices, which can improve the quality of a patient's health and reduce healthcare costs. The FDA and FCC chairman signed a joint statement of principles and memorandum of understanding at the start of a two-day conference, which began July 26, to showcase a broad range of cutting-edge wireless medical devices as well as discuss issues affecting the telehealth industry. The joint statement declared that healthcare providers, patients, and other stakeholders "should have clear regulatory pathways, processes, and standards to bring broadband

and wireless-enabled medical devices to market. This includes clarity regarding each agency's scope of authority with respect to these devices, predictability regarding regulatory pathways, and streamlining the application process, as appropriate, to facilitate innovation while protecting patients." Source: http://www.informationweek.com/news/healthcare/leadership/showArticle.jhtml?articleID=226300045&subSection=All+Stories

FCC plan to support emergency communications relies on unproven technology. A proposal to auction 10 megahertz of broadband spectrum to commercial organizations, rather than dedicating the spectrum exclusively for public safety communications, relies on unproven technology to provide first responders priority access, a Homeland Security Department official told Congress July 27. The Federal Communications Commission's (FCC) National Broadband Plan, released in March, includes a proposal to auction the 10 megahertz of spectrum known as D-Block to commercial interests, providing public safety organizations priority access in emergency events with next-generation wireless broadband technologies that — while unproven — promise to increase the capacity and speed of mobile telephone networks. "The technology being recommended by the FCC provides great opportunity," said the assistant secretary of the Office of Cybersecurity and Communications at DHS during testimony before the House Subcommittee on Emergency Communications, Preparedness and Response. "It's not absolutely clear what [this technology] is capable of." Homeland Security would support FCC's plan for the auction if the technical and legal frameworks were properly evaluated, and the technology's capacity and capability were understood to meet public safety requirements, he added. Many public safety organizations oppose the proposal to auction the D-Block spectrum to commercial interests, instead supporting a bill that would dedicate the spectrum to public safety. Source: http://www.nextgov.com/nextgov/ng_20100727_6546.php

Critical Manufacturing

(Ohio) **Alcoa evacuated after bomb scare.** A Cuyahoga Heights, Ohio Alcoa Plant was evacuated July 28 because of a bomb threat. According to police, a bomb was thought to be in the bathroom facility of the plant. At 8:24 a.m., police evacuated the building and swept the facility. No bomb was found and employees were allowed to return to work. The Cuyahoga Heights Police Department is still investigating the incident. Source: http://www.newsnet5.com/dpp/news/local_news/alcoa-evacuated-after-bomb-scare

Toyota recalls Avalons to correct steering defect. Toyota has recalled approximately 373,000 2000-2004 Model Year Toyota Avalons sold in the United States because the vehicle's steering lock bar could break under certain conditions. No other Toyota or Lexus vehicles are involved in this recall. Toyota said there was improper casting of the steering lock bar, which is a component of the steering interlock system. That defect, Toyota noted, creates the possibility that a minute crack may develop on the surface. Such a crack may expand over a long period of repeated lock and unlock operations, and eventually the lock bar could break. If this occurs, the interlock system may become difficult to unlock when stationary. If the vehicle — while being driven — is steered to the right with sufficient lateral acceleration, a broken and loose lock bar may move toward the steering shaft. If the engagement hole in the shaft happens to line up at the specific time the broken lock bar has moved, this could cause the steering wheel lock bar to engage, locking the steering wheel, and increasing the risk of a crash. As part of the recall, Toyota will replace the steering column bracket, a procedure that

takes about two hours to complete depending on the dealer's schedule. Toyota will notify owners by first class mail beginning in late August 2010 to bring their vehicles to their local dealer for replacement of the steering column bracket at no charge to the customer. Source: http://www.consumeraffairs.com/news04/2010/07/toyota_steering_recall.html

2009-2010 Nissan Cubes recalled. Nissan is recalling some 2009-2010 Cubes after a test vehicle leaked more than the allowable amount of fuel following a crash test. Excessive fuel leakage can cause a fire. Dealers will attach a protector tube to the gasoline recirculation tube when the recall begins in August. Source: http://www.consumeraffairs.com/recalls04/2010/nissan_cube.html

DEFENSE/ INDUSTRY BASE SECTOR

Report: Ability to ID nukes fading. The National Research Council says the ability of U.S. intelligence to confidently identify the source of nuclear weapons used in a terrorist attack is eroding. "Although U.S. nuclear forensics capabilities are substantial and can be improved, right now they are fragile, under-resourced and, in some respects, deteriorating," the council said in its report, "Nuclear Forensics: A Capability at Risk," released July 29. Nuclear forensics amounts to specialized detective work in which scientists identify the radioactive components of nuclear devices, finding and tracing the materials to clarify options for retaliation, The New York Times said. A clear ability to determine which attacker used what atomic material from fallout and debris after an attack is considered a deterrent against nuclear terrorism. But the report, prepared by nuclear specialists from the military, industry and academia, said old facilities, outdated equipment and a lack of skilled personnel are eroding nuclear forensic capabilities. The study was requested by the Defense Department, the Department of Homeland Security, and the National Nuclear Security Administration, a part of the U.S. Department of Energy. Source: http://www.upi.com/Top_News/US/2010/07/29/Report-Ability-to-ID-nukes-fading/UPI-24211280438760/

(Michigan) **2 diagnosed with Legionnaires' disease.** Two workers at a Michigan Air National Guard base were diagnosed with Legionnaires' disease. Twenty-nine employees were diagnosed and six hospitalized with upper respiratory illnesses between July 12 and July 24 at Selfridge Air National Guard Base in suburban Detroit, according to a July 27 press release. An airman and a civilian worker have since been diagnosed with Legionnaire's disease, a bacterial infection that can lead to high fever, chills and a cough. Between 8,000 and 18,000 people are hospitalized each year with the disease, according to the Centers for Disease Control and Prevention. Two buildings have been cleaned and sanitized, the air-conditioning units have been serviced and sanitized, and the cooling tower was treated with a disinfectant. Air- and water-quality test results are pending. The buildings are home to offices of the Army Tank-automotive and Armaments Command's Life Cycle Management Command. Source: http://www.airforcetimes.com/news/2010/07/airforce_michguard_072810w/

(Iowa) **Bomb found at Waterloo plant has no explosives.** A bomb found in a former munitions plant in Waterloo, Iowa is safe, police said July 23. Workers demolishing the plant found the bomb on a water heater July 21. A Waterloo police investigator said a team from Fort Leonard Wood has determined there were no explosives inside the device, and that the bomb is a warhead for a Nike-Hercules missile. The warhead will be taken to Fort Leonard Wood. The plant closed 16 years ago and currently is being torn down. Source:

http://www.desmoinesregister.com/article/20100724/NEWS/100723041/-1/WATCHDOG/Bomb-found-at-Waterloo-plant-has-no-explosives

Emergency Services

(California) **Agencies drill for nuclear terrorist attack.** Firefighters, police, sheriff's deputies, paramedics, the county coroner and other emergency services personnel will participate in a TRAINING exercise today that simulates a response to the detonation of 10-kiloton improvised nuclear device. The drill is not based on any actual intelligence information or threat to Los Angeles or the United States, a spokesman for the county's Office of Emergency Management. It is geared toward advance planning for such an event and to share information and technology between first responders and public safety personnel at local, state and federal levels. Such an improvised nuclear device could be small enough to be carried in a briefcase, but would wreak "indescribable" devastation. After detonation, depending on wind patterns, a plume cloud could cover much of the Southern California area. Source: http://www.contracostatimes.com/california/ci_15621090?nclick_check=1

(Florida) **2 arrested after acid bombs thrown at cops' homes.** Volusia County, Florida, deputies say two young men threw acid bombs at the homes of two law enforcement officers in Deltona on July 26 in the night. Investigators say one of the homes belongs to a Volusia County deputy and the other is the home of a Lake Mary police officer. It is unclear at this point why law enforcement was the target in both of these attacks, but no one was injured. Police have not released the names of the two young men who have been arrested for allegedly detonating acid bombs. One 25-year-old suspect had nothing to say to a WFTV news crew as he was taken away for questioning, but what investigators found at his home is telling. Crime Scene Investigators picked through a stockpile of plastic jugs. One neighbor says they saw the suspects and chased them. Within minutes, SkyWitness 9-HD was overhead and recorded an arrest. It is still unclear why the suspects targeted these two specific homes. It is also unclear what chemicals exactly were used to make the bombs. Source: http://www.wftv.com/news/24402526/detail.html

(Alaska) **Alaska delegation asks feds to replace lost Coast Guard helicopter.** Alaska's congressional delegation has sent a letter to the Department of Homeland Security Secretary, requesting funding to replace a lost Coast Guard helicopter. The MH-60 Jayhawk helicopter assigned to Air Station Sitka crashed earlier this month off La Push, Washington, killing three crewmen. "Alaska has more coastline than any other state in the nation. The loss of a helicopter from Air Station Sitka reduces the ability of the Coast Guard to respond to maritime emergencies and places Alaska's commercial and recreational boating public at increased risk," the delegation said in the letter. The Coast Guard has said it will temporarily shift a helicopter to Sitka from the Lower 48, but the delegation argues that moving a chopper from another location will only create an additional resource gap elsewhere. Source: http://www.ktuu.com/Global/story.asp?S=12857979

Energy

Smart meters pose hacker kill-switch risk, warn boffins. A professor in security engineering at the University of Cambridge Computer Laboratory warns that the move to smart metering introduces a

"strategic vulnerability" that hackers might conceivably exploit to remotely switch off elements on the gas or electricity supply grid. A program is underway to replace Britain's 47 million meters with smart meters that can be turned off remotely. The off switch creates information security problems of a kind, and on a scale, that the energy companies have not had to face before. From the viewpoint of a cyber attacker –- whether a hostile government agency, a terrorist organization or even a militant environmental group –- the ideal attack on a target country is to interrupt the electricity supply. The combination of commands that will cause [smart] meters to interrupt the supply, of applets and software upgrades that run in the meters, and of cryptographic keys that are used to authenticate these commands and software changes, create a new strategic vulnerability. Smart meter roll-outs are taking place in both the U.S. and Europe, with other regions likely to follow. The Cambridge team warns that either software error, possibly during a system update, or a hacker taking seizing control of smart meter systems (perhaps via some form of cryptographic attack) could have a devastating effect. Source: http://www.theregister.co.uk/2010/07/28/smart_meter_security_risks/

(Vermont) **Suspicious Barre rail car fire under investigation.** A suspicious fire is under investigation in Barre, Vermont. At around 6 p.m. July 25 fire officials responded to a small fire near the railroad tracks off Depot Square. They say they found a burning box spring propped up against a rail car. However that rail car was filled with heating oil. Crews put a quick stop to the blaze but say, given the circumstances, there was never a serious threat of an explosion. Source: http://www.wcax.com/Global/story.asp?S=12874975

(Maryland; Virginia; District of Columbia) **More than 240,000 still without power.** More than 300,000 people lost power in the greater Washington D.C. metropolitan area after powerful thunderstorms ripped through July 25 knocking down trees and wires.. As of about 9:45 a.m. July 26, Pepco reported more than 230,000 homes without power in Maryland and Washington D.C.. The vast majority are in Montgomery County, Maryland where more than 173,000 homes still lack power. Dominion recorded nearly 12,000 homes without power in northern Virginia the morning of July 26. Mandatory water restrictions are still in effect for Washington Suburban Sanitary Commission customers in Montgomery and Prince George's counties in Maryland. At least two deaths were reported during the July 25 storm. A woman was killed in Beltsville, Maryland when a tree fell on her minivan, and a 6-year-old boy died in Sterling, Virginia after a tree fell on him. Source: http://www.washingtonexaminer.com/local/blogs/capital-land/more-than-240000-still-without-power-99232649.html

Food and Agriculture

Dairy farms misuse antibiotics. E. coli bacteria have already shown some resistance to gentamicin, a heat-stable antibiotic. And sulfamethazine, a sulfonamide antibacterial, is one of the most common animal drugs used on dairy farms. The U.S. Food and Drug Administration (FDA) has not established any tolerance level for gentamicin in the edible tissues of veal calves. But when checking up on a bob veal calf sold at a dairy farm at Cassadaga, New York, tissue samples returned residues of gentamicin in the liver, kidney, and muscle tissue of the animal. In a July 9 warning letter, FDA said the presence of the drug in the edible tissue of the animal causes the food to be adulterated under federal law. "Our investigation also found that you hold animals under conditions that are so inadequate that medicated animals bearing potentially harmful drug residues are likely to enter the food supply," FDA said in the letter. The agency told the man his treatment records are not be properly maintained, and

the dairy farm is using Gentamicin Sulfate in ways not provided for on its label. Such "extra label" use of an animal drug is allowed only under the supervision of a licensed veterinarian. Meanwhile, a Maple Park, Illinois dairy farm received a warning letter from the FDA about its alleged misuse of the animal drug sulfamethazine. The owners sold a dairy cow for slaughter as food, according to FDA, that had 2.649 parts per million (PPM) of sulfamethazine residue in the liver tissue. The FDA established tolerance of 0.1 ppm for residues of sulfamethazine in the uncooked edible tissue of cattle. In the letter, FDA said the Hills "did not use sulfamethazine boluses as directed by the approved labeling." The label instructions for the drug clearly state that it is not to be used for female dairy cattle 20 months of age or older. USDA's Food Safety and Inspection Service (FSIS) did the tissue sampling for both the bob calf and the dairy cow. Some fear animal antibiotics in food are making some antibiotics in humans ineffective. Source: http://www.foodsafetynews.com/2010/07/dairy-farms-misuse-antibiotics/

(Wisconsin) **Five Wisconsin counties now confirmed to have late blight.** A plant pathologist with the University of Wisconsin-Extension said late blight has been confirmed in five Wisconsin counties. On July 23, late blight was confirmed on potatoes in Portage County, and on tomatoes in Monroe and Kewaunee Counties. Initial studies indicated that the late blight strain from potatoes will infect tomatoes and the strain from tomatoes will infect potatoes. The late blight pathogen is referred to as a water mold since it thrives under wet conditions. Symptoms of tomato late blight include leaf lesions beginning as pale green or olive green areas that quickly enlarge to become brown-black, water-soaked, and oily in appearance. Lesions on leaves can also produce pathogen sporulation which looks like white-gray fuzzy growth. Stems can also exhibit dark brown to black lesions with sporulation. Tomato fruit symptoms begin small, but quickly develop into golden to chocolate brown firm lesions or spots that can appear sunken with distinct rings within them; the pathogen can also sporulate on tomato fruit giving the appearance of white, fuzzy growth. With the presence of the late blight pathogen in the state and disease-favorable weather conditions, it is critical that all growers of tomatoes and potatoes regularly scout their plants for disease symptoms. Source: http://www.wisconsinagconnection.com/story-state.php?Id=872&yr=2010

ESPN calls foul on sports chow. Entertainment Sports Programming Network's (ESPN) "Outside the Lines" television program took a look at health department inspection reports at 107 professional sports stadiums, and according to the data, the Tampa Bay Rays' Tropicana Field and the Washington Wizards' Verizon Center were the top offenders, as every single food and drink vendor at each stadium received a critical violation in the last year. Critical or major violations include food temperature, cross-contamination, hygiene, equipment and rodent or insect contamination, according to ESPN. The report is careful to point out that so far, food served at professional sports stadiums have never been linked to a mass food-borne illness outbreak. Source: http://www.nbclosangeles.com/around-town/food-drink/ESPN-Stadium-Health-Inspections-California-99334804.html

Report: Imported catfish human health risk. According to a report from Exponent Inc.'s Center for Chemical Regulation and Food Safety, eating contaminated catfish imported from Vietnam and China could have "serious long-term human health consequences." The report cites "major hazards" associated with aquaculture fish, including pathogenic microorganisms, antimicrobial drug residues, and environmental chemicals. The chairwoman of the Senate Agriculture Committee, joined the group, Food & Water Watch, and the Catfish Farmers of America in unveiling the report July 22 on

Capitol Hill. She said she had been "loud and clear" on the U.S. Department of Agriculture's (USDA's) delay in implementing the catfish inspection rule, part of the 2008 Farm Bill, which shifted jurisdiction over catfish safety from the Food and Drug Administration (FDA) to the USDA's Food Safety and Inspection Service (FSIS). The rule has yet to be implemented. The proposed rule has languished in the Office of Management and Budget reportedly because of objections raised by the Office of the U.S. Trade Representative over concerns that countries currently exporting catfish to the U.S. may not be able to meet the food safety standards FSIS would require. Source: http://www.foodsafetynews.com/2010/07/report-imported-catfish-human-health-risk/

Government Sector (including Schools and Universities)

US closes consulate in Mexico's Ciudad Juarez. The United States has closed indefinitely its consulate in the violence-hit Mexican city of Ciudad Juarez while it carries out a "security review," officials said July 30. "The US consulate general in Ciudad Juarez has closed to review its security posture," said a statement released by the US embassy in Mexico City. "The facility will be closed all day on Friday, July 30, and remain closed until the security review is completed." US officials added: "American citizens are advised avoid the area around the consulate general until it reopens." Source: http://www.google.com/hostednews/afp/article/ALeqM5hxvX5IgybeHFgNGVexB0gbscM0gw

U.S. Paris embassy staff tested after handling suspicious mail. Two employees of the U.S. embassy in France are undergoing medical tests at a Paris hospital, after they handled a "suspicious" envelope. "The two employees who were exposed to it were evaluated by medical professionals," said a spokeswoman for the U.S. State Department in Washington D.C. Early results indicate that the envelope is not harmful, said the embassy's deputy spokeswoman. The anti-terrorist unit of Paris's police, which usually treats such cases, was not called in, a police official said, adding that the embassy may have decided to handle it internally or that the incident may not have been serious enough. He declined to be named in line with police rules. The envelope was sent to a laboratory for analysis, the deputy spokeswoman said. She said she didn't have details on the origins of the envelope or to whom it was addressed. The two employees were French nationals who work for the embassy, she said, adding that she had no details on the symptoms they showed. The embassy was not evacuated. Source: http://www.businessweek.com/news/2010-07-30/u-s-paris-embassy-staff-tested-after-handling-suspicious-mail.html

(Alaska) **4 killed in plane crash at Alaska military base.** Authorities said all four airmen aboard a C-17 that crashed at an Air Force base in Alaska were killed. The spokesman said three of the men were in the Alaska Air National Guard and the fourth was on active duty at Elmendorf Air Force Base. Their names have not been released pending notification of relatives. The plane was on a local training run July 28 when it crashed. Witnesses said the crash sent a fireball rising hundreds of feet over the base near downtown Anchorage. Source: http://www.google.com/hostednews/ap/article/ALeqM5jw-r3K3LaOaVY5UIUH6EWiAUia6gD9H8N7RG2

(Alabama) **Sheriff's office: Courthouse bomb threats could be related.** The Houston County Sheriff's Office said they are investigating the possibility two recent bomb threats in Dothan, Alabama are related. On July 23, a man called the court clerk's office claiming there was a bomb in the Houston County Courthouse. The building was evacuated and searched — but nothing was found. Then a

similar situation occurred July 26 — only this time the call was made to Dothan Police. Again, nothing was found. Deputies said the back to back threats are suspicious and could be related. They are working to trace the source of the felony hoaxes. Source: http://dothanfirst.com/fulltext/?nxd_id=117715

(Oklahoma) **City building evacuated Friday.** City of Norman Building Complex A was evacuated for about 30 minutes on the morning of July 23 as police investigated a suspicious package. A Norman Police captain said police were told about the situation about 9:40 a.m. July 23. Reports indicated that a man placed a package near the north side doors and rode off on a bicycle. The captain said NPD's Hazardous Devices Unit and University of Oklahoma Police Department responded. When officers arrived, they found a bag and blanket near the doors. Officers found the bag and blanket's owner a short distance away at the Norman Public Library. The man opened the bag for police. Nothing hazardous was found inside the bag, the captain said. Employees were allowed back inside the building a short time later. Source: http://normantranscript.com/headlines/x1079908796/City-building-evacuated-Friday

(Maryland) **Man charged in courthouse bomb threat.** Maryland State police have served an arrest warrant on a man, charging him with making a bomb threat in May against the District Courthouse in Westminster. The suspect was served the warrant on July 23. He is being held at the Baltimore County Detention Center on an unrelated charge. On May 12, a court employee received a call that there was a bomb in the courthouse. District and Circuit courts were evacuated, but a search did not find explosive devices. Source: http://wjz.com/local/maryland.courthouse.bomb.2.1825839.html

(Pennsylvania) **Fire set at recruiting office.** Someone tried to light the door of the Marine Corps recruiting office on fire in what police say appears to be the latest in a string of suspicious fires. State College police say an interior door to the center was minimally damaged by the attempt. The center is on the ground floor of 242 S. Fraser St., and above it are several floors of apartments. To get to the door, police said the suspects would have had to enter the building. A State College police lieutenant said that concerns police, because even if a business on the bottom floor was the target, a fire on the first floor poses a big risk to the residents of the apartments above. So far, the rash of suspicious blazes have been classified as nuisance fire — those set outdoors or at vacant buildings. This one "can't be classified as a nuisance fire because it's an occupied structure, there's a possibility that people would be hurt," the lieutenant said. "It creates even more of a danger to the firefighters that might respond to something like that, because they have a concern of evacuating people as well as fighting a fire on a structure is much more dangerous than an external pile of wood or unoccupied property." Source: http://www.centredaily.com/2010/07/24/2111715/fire-set-at-recruiting-office.html

NATO allies fear fallout of leaked Afghan war docs. Several European NATO members have expressed concern that the fallout from a massive online leak of confidential U.S. documents on the Afghan war could extend well beyond the Internet — and could even affect the war itself. The U.S. records cover six years of the war in Afghanistan, including previously unknown accounts of civilian deaths and targeted attacks on Taliban members. "A lot of it is mundane, but a lot of it is also very serious, on-the-ground, battlefield reports about the situation in the war, and right now it doesn't seem like it is matching the narrative that is coming out of the Pentagon," a freelance journalist told CTV's Canada AM during an interview in Toronto July 26. Some reports, for example, reveal that the

Taliban "apparently have surface-to-air missiles, which contradicts everything we've heard from the Pentagon about the kind of weaponry that's being seen in the field," said the journalist, who has reported in Afghanistan in the past. So far, NATO has declined comment on the release of the U.S. documents. But representatives from NATO member countries said they hope the leaks do not pose problems for the current war effort. The German foreign minister warned that "backlashes" could result from the 91,000 records posted online by the WikiLeaks organization July 25. The British foreign secretary said that with recent progress being made in Afghanistan, he hoped "any such leaks will not poison that atmosphere." Source: http://www.ctv.ca/CTVNews/World/20100726/wikileaks-nato-concerns-100726/

Information Technology and Telecommunications

'Unhackable' Android phone can be hacked. Suspect software cloaked in a wallpaper application has gathered personal information from infected Android phones and sent it to a Web site in China, and researchers from Lookout Mobile Security have found a way to take the Android over completely – including top-of-the-line models hawked by major wireless carriers. In one presentation at Black Hat 2010, Lookout's CEO said the Jackeey Wallpaper app, which has been downloaded millions of times, can gather a device's phone number, subscriber identifier, and currently programmed voicemail number. In a separate presentation, researchers said top-of-the-line Android phones used by Sprint and Verizon can be taken over completely by attacking known flaws in the Linux operating system that underpins Android, researchers reported at Black Hat 2010. "It gives you root control, and you can do anything you want to do" with the phone, says a researcher for Lookout Mobile Security. The best way to distribute malware that could exploit the flaw – known as CVE-2009 1185 – is via Android applications that customers might acquire free or buy from the Android Market. Installing the booby-trapped application would give root control of the device. CVE-2009 1185 has been known for more than a year and can be patched, but so far the carriers have not issued patches. The root-control exploit has been successfully carried out in Lookout labs on EVO 4G (Sprint), Droid X (Verizon), and Droid Incredible (Verizon) as well as older models G1 and Hero. But root control is unnecessary in order to carry out the type of attack executed by Jackeey Wallpaper, according to another Lookout researcher. Applications require permissions in order to access features of the phone, and these permissions can be exploited. So, for instance, an application that tells the customer the nearest Chinese restaurant would need access to the phones GPS capabilities. Source: http://www.networkworld.com/news/2010/072910-black-hat-android-hack.html?hpg1=bn

Verizon: Data breaches often caused by configuration errors. Hackers appear to be increasingly counting on configuration problems and programming errors rather than software vulnerabilities in order to steal information from computer systems, according to a new study from Verizon. Verizon said it found that a surprising and "even shocking" trend is continuing: There are fewer attacks that focus on software vulnerabilities than attacks that focus on configuration weaknesses or sloppy coding of an application. In 2009, there was not a "single confirmed intrusion that exploited a patchable vulnerability," the report said. The finding has caused Verizon to question whether patching regimes — while important — need to be done more efficiently given the trend in how attacks are occurring. In other findings, some 97 percent of the malicious software found to have stolen data in 2009 was customized in some way. Source: http://www.computerworld.com/s/article/9179848/Verizon_Data_breaches_often_caused_by_configuration_errors

100 million Facebook accounts exposed. The details of 100 million Facebook users have been posted online by a security analyst, in a stark demonstration of the potential privacy weaknesses of social networks. In a detailed blog post, an analyst from Skull Security explained that he used a simple piece of code to perform the scrape, which took any data not already locked down within personal privacy settings. However, as of the morning of July 29, his Web site and the blog post were unavailable. The list of users has been shared on peer-to-peer site The Pirate Bay, and included in the packaged files are names and Facebook URLs. Facebook explained that the information that was taken had already been made public by users. However, the firm is investigating whether the collection of information in this way was a violation of its terms and conditions. A senior technology consultant at security firm Sophos concurred with Facebook's stance, explaining that it was enabled by lax user controls. He said he hoped the incident would prompt social network users to harden their security settings. Source: http://www.v3.co.uk/v3/news/2267280/fifth-facebook-accounts-exposed?page=1

Critical vulnerability in Apple QuickTime. A highly critical vulnerability affects the latest version of Apple QuickTime Player for Windows. "The vulnerability is caused due to a boundary error in QuickTimeStreaming.qtx when constructing a string to write to a debug log file," said a Secunia researcher. "This can be exploited to cause a stack-based buffer overflow by e.g. tricking a user into viewing a specially crafted web page that references a SMIL file containing an overly long URL." If the flaw is successfully exploited, arbitrary code can be executed by the attacker, and the system can be compromised. So far, the vulnerability is confirmed to affect only the latest version of the software (7.6.6) for Windows, which was released March 30. Source: http://www.net-security.org/secworld.php?id=9649

Twitter and Google are riddled with malicious links. Almost three quarters of Twitter's 100 million accounts are unused or responsible for delivering malicious links. The 2010 mid-year security report from Barracuda Labs analyzed more than 25 million Twitter accounts, both legitimate and malicious, and found that true Twitter users (a user that has at least 10 followers, follows at least 10 people, and has tweeted at least 10 times) tweet more often, and as casual users become more active, malicious activity increases. Only 28.87 percent of Twitter users are "true Twitter users,"and the Twitter crime rate — the percentage of accounts created per month that were eventually suspended for malicious or suspicious activity, or otherwise misused — for the first half of 2010 was 1.67 percent. Google distributed the most malicious links of four of the most popular online services Bing, Twitter, and Yahoo, with 69 percent of its results poisoned when searches on popular trending topics were performed. The analysis reviewed more than 25,000 trending topics and nearly 5.5 million search results. Source: http://www.scmagazineuk.com/twitter-and-google-are-riddled-with-malicious-links/article/175673/

WPA2 vulnerability found. Wireless security researchers say they have uncovered a vulnerability in the WPA2 security protocol, which is the strongest form of Wi-Fi encryption and authentication currently standardized and available. Malicious insiders can exploit the vulnerability, named "Hole 196" by the researcher who discovered it at wireless security company AirTight Networks. The moniker refers to the page of the IEEE 802.11 Standard (Revision, 2007) on which the vulnerability is buried. Hole 196 lends itself to man-in-the-middle-style exploits, whereby an internal, authorized Wi-Fi user can decrypt, over the air, the private data of others, inject malicious traffic into the network and compromise other authorized devices using open source software, according to AirTight. The

Advanced Encryption Standard (AES) derivative on which WPA2 is based has not been cracked and no brute force is required to exploit the vulnerability. Rather, a stipulation in the standard that allows all clients to receive broadcast traffic from an access point (AP) using a common shared key creates the vulnerability when an authorized user uses the common key in reverse and sends spoofed packets encrypted using the shared group key. Source: http://www.pcworld.com/article/201822/wpa2_vulnerability_found.html

Zeus bot latches onto Windows shortcut security hole. Miscreants behind the Zeus cybercrime toolkit and other strains of malware have begun taking advantage of an unpatched shortcut handling flaws in Windows. It was first used by a sophisticated worm to target SCADA-based industrial control and power plant systems. Zeus-contaminated emails pose as security messages from Microsoft, containing contaminated ZIP file attachments laced with a malicious payload that utilises the lnk flaw to infect targeted systems. Several additional malware families have also latched onto the same Windows shortcut trick including Sality, a popular polymorphic virus. Trend Micros confirms the appearance of the exploit vector in variants on Zeus and Sality while McAfee adds that the VXers behind the Downloader-CJX Trojan have also begun feasting off the shortcut security bug. Fortunately virus writers are, thus far at least, using the same basic exploit method, a factor that makes it easier for security firms to block attacks. Microsoft is advising users to apply temporary workarounds while its security researchers investigate the shortcut flaw, a process likely to eventually result in a patch. Source: http://www.theregister.co.uk/2010/07/27/zeus_exploit_shortcut_hole/

Iran was prime target of SCADA worm. Computers in Iran have been hardest hit by a dangerous computer worm that tries to steal information from industrial control systems. According to data compiled by Symantec, nearly 60 percent of all systems infected by the worm are located in Iran. Indonesia and India have also been hard-hit by the malicious software, known as Stuxnet. Looking at the dates on digital signatures generated by the worm, the malicious software may have been in circulation since as long ago as January, said a senior technical director with Symantec Security Response. Stuxnet was discovered last month by VirusBlokAda, a Belarus-based antivirus company that said it found the software on a system belonging to an Iranian customer. The worm seeks out Siemens SCADA (supervisory control and data acquisition) management systems. Siemens would not say how many customers it has in Iran, but the company now says that two German companies have been infected by the virus. A free virus scanner posted by Siemens the week of July 19 has been downloaded 1,500 times, a company spokesman said. Source: http://www.computerworld.com/s/article/9179618/Iran_was_prime_target_of_SCADA_worm?taxonomyId=85

New report: Apple software has the most vulnerabilities. A new report from security software provider Secunia finds that the latest data shows Apple has surpassed Oracle and even Microsoft with accounting for the most software vulnerabilities, though the No. 1 ranking is related only to the number of vulnerabilities — not to how risky they are or how fast they get patched. The report offers support to the notion that a high market share correlates with a high number of vulnerabilities. Since Mac OS accounts for only a small share of the market, hackers have largely stayed away from it, probably figuring that the potential for obtaining lucrative private information would be less rewarding than the information that could be had by attacking Windows-based system. Source: http://homelandsecuritynewswire.com/new-report-apple-software-has-most-vulnerabilities

National Monuments and Icons

(Montana) **Bear kills man, injures two near Yellowstone Park.** One man was killed and a man and a woman were injured by bear attacks in the middle of the night July 28 at a popular campground on the edge of Yellowstone Park in Montana, wildlife officials said. A Montana Fish, Wildlife and Parks Department spokesman said it was believed one bear was involved and at least two tents were left in tatters in the attack, which occurred at the height of the tourist season. He said the attacks appeared to be unprovoked, and that the presence of food, which often attracts bears and other wildlife into campgrounds, did not appear to be a factor. Such "random predatory" bear attacks on humans are rare, he said. Soda Butte in Cooke City, Montana, which offers 27 campsites in a national forest known for its blue-ribbon trout fishing, was immediately evacuated and nearby campgrounds were closed after the attacks. The incident occurred at the height of the tourist and camping season. Wildlife officials launched an all-out search for the bear, or bears, including the use of airplanes and helicopters on the lookout for radio-collared animals or others in the vicinity. Bear traps also were being set in the campground. An investigation was underway to piece together events. Source: http://www.reuters.com/article/idUSTRE66R5VK20100728?type=domesticNews

(California) **Wildfires spark state of emergency in California county.** Kern County, California was under a state of emergency July 28 as a result of spreading wildfires that have destroyed 25 homes, caused more than 2,300 people to evacuate and burned 15,000 acres. The afternoon of July 27, firefighters were called to a new wild fire southeast of Tehachapi. Later that night the fire had grown, threatening 150 structures, authorities reported. Fire crews battled through the night with aircraft, fire engines, and bulldozers. Crews worked throughout the night protecting homes and trying to contain the blaze. An evacuation center was set up at the old junior high school nearby for evacuees and their pets. Animal control was taking large animals, authorities said. In addition, more than 1,000 firefighters continued to battle a blaze July 28 in California's Sequoia National Forest, north of Tehachapi. As of July 27, that fire had spread across roughly 6,000 acres, a U.S. Bureau of Land Management spokeswoman said. The bureau is working with the U.S. Forest Service and the Kern County Fire Department to fight the blaze. Kern County is approximately 130 miles north of Los Angeles. Source: http://www.cnn.com/2010/US/07/28/california.wildfires.spread/

(Wyoming) **Fire in Yellowstone 72% contained.** Firefighters are making progress containing a blaze burning near the center of Yellowstone National Park in Wyoming. The fire has burned about 520 acres and is now 72 percent contained. Firefighters July 26 plan to put out spot fires burning along the northern edge of the fire. Helicopters will continue to help put out the fire from the air. The weather could cause problems later in the day when thunderstorms and gusty winds are expected. Source: http://www.khq.com/Global/story.asp?S=12866062

Postal and Shipping

(Kentucky) **Explosives set off in Kentucky neighborhood.** In all, four explosions rocked Pikeville, Kentucky July 27. Two homes had mailboxes blown apart. Pikeville police said the suspects planted a third device in the Pikeville City Park. A Pikeville Police detective said a fourth bomb exploded right outside the Pike County Courthouse. Investigators can not be sure of a motive, but they believe this may have been simply a very bad idea for a prank. Still, police said these are serious crimes, and those responsible will be facing serious consequences. Police said they are working with prosecutors

to determine all the charges the people responsible should face but said they will likely include felony charges of possession of a destructive device. Source: http://www.wkyt.com/news/headlines/99504489.html?ref=489

(Masachusetts) **White powder remains a mystery.** The white power that contaminated a resident of Patriots Road in Templeton, Massachusetts is not toxic and is not a biological agent, the town police chief said, but it's still unknown what it is. The chief said the state department of public health is conducting further tests in the hope of finding out exactly what was in the envelope in the mail that a resident opened July 27 at his home. When a powdery substance got on the man's face and caused a burning sensation to his eyes and face, he called police. He was treated and did not develop further problems. The state department of fire services hazardous materials unit and the state police were called to investigate. On July 27, police and fire services personnel were unable to determine what the substance was, and the powder and the envelope were taken to the public health lab to be examined. The police chief said there was a handwritten note inside the envelope, but that he had not been able to examine it. "Hopefully, it will shed some light on this," he said. The envelope is being checked for fingerprints by the state police crime lab. No arrests have been made, and police are not speculating about possible suspects. Source: http://www.telegram.com/article/20100729/NEWS/7290691/1101

(Virginia) **Explosive devices left in mailboxes in Orange.** The Orange County Sheriff's Office is investigating a string of homemade explosives put into mailboxes on Raccoon Ford Road in Burr Hill, Virginia. The devices were put in five mailboxes July 26, according to officials. Authorities including the Virginia State Police bomb squad and a state hazardous materials team removed the devices, which detonated but caused little to no damage, according to officials. A stretch of the road was shut down for more than four hours while the items were removed. The sheriff's office asks that anyone with information about the vandalism to call (540) 672-1200. Source: http://www2.dailyprogress.com/news/2010/jul/27/explosive-devices-left-mailboxes-orange-ar-352254/

(Virginia) **Suspicious envelopes force evacuation of Henrico office building.** Authorities evacuated a Glen Allen, Virginia office building at 4551 Cox Road in Henrico County July 27, after two envelopes deemed suspicious were delivered to a second-floor attorney's office within an hour, police said. The Henrico Division of Police's bomb squad was called at 10:45 a.m. after the recipient of the two envelopes did not recognize the return addresses — one from Connecticut, the other from Massachusetts, said a Henrico police spokesman. A Henrico fire & EMS hazardous materials team was also summoned to the scene. As a precaution, building occupants were evacuated to the parking lot while authorities tried to determine the content of the envelopes, the spokesman said. The building's first floor contains the legislative offices of a senator, but authorities do not believe the potential threat was directed at him. The spokesman said the U.S. Postal Service delivered the two envelopes within an hour's time. Source: http://www2.timesdispatch.com/news/2010/jul/27/coxxgat27-ar-351910/

(Massachusetts) **Man opens mail, finds white powder.** In Templeton, a white powdery substance a Patriots Road resident was exposed to when he opened his mail on the afternoon of July 26 is expected to be taken July 27 to the state Department of Public Health for testing to determine if it is hazardous. The Police Chief said July 26 that the resident suffered irritation to his eyes and face after

opening a letter he had collected from his mailbox about 1:15 p.m. The Chief said an unknown white powder is believed to have caused the irritation. The resident rinsed his face with water while calling police. Police and emergency services people helped the resident further rinse his face and gave him oxygen because he was having some breathing difficulty. The state Department of Fire Services Hazardous Materials Unit and investigators from the State Police Crime Prevention and Control Unit and the U.S. Postal Service were helping assess the material from the letter, which Police dropped outside his house. Source: http://www.telegram.com/article/20100727/NEWS/7270377/1003/NEWS03

PUBLIC HEALTH

FDA finds problems at Sanofi vaccine plant. Food and Drug Administration (FDA) inspectors visited a plant operated by Sanofi Pasteur, the company's vaccine unit, in Marcy l'Etoile, France, in March and April, the agency's July 22 letter to the company said. Inspectors found the company did not comply with federal manufacturing standards in the production of the Typhim Vi typhoid vaccine, the Imovax rabies vaccine and other products, the letter said. The company said its products on the market were safe and effective. "We either have already addressed the issues raised or are currently working diligently to address them," the Sanofi Pasteur chief executive said in a written statement. The company's vice president of industrial operations, said he was confident the issues raised by the FDA could be corrected "in a timely way." He said he did not expect vaccine supply to be disrupted. Source: http://www.reuters.com/article/idUSTRE66S62D20100729

(Texas) **Texas sees whooping cough cases rise.** As California faces one of the state's worst whooping cough outbreaks in more than 50 years that has resulted in six infant deaths and 1,500 confirmed infections, Texas health department officials have now begun reporting increases in whooping cough infections. The biggest increase in infections, NBCDFW.com reports, is in central Texas, with more infections reported in Tarrant County in north Texas. Dallas County has not reported an increase in whooping cough cases. Numbers are not high enough yet to declare an epidemic or outbreak. According to state health department statistics, the number of whooping cough cases has risen by almost 60 percent in Texas since 2008. Investigators from the health department are closely monitoring all reported cases. The whooping cough vaccination is usually administered in a combination shot that also provides protection against tetanus and diphtheria. Source: http://vaccinenewsdaily.com/news/214357-texas-sees-whooping-cough-cases-rise

(California) **California whooping cough outbreak largest in decades.** Nearly 1,500 Californians this year have been diagnosed with whooping cough — five times the normal level for this time of year, state health officials said. Doctors are investigating another 700 possible cases. Many more people may have had the infection, which often goes undiagnosed or unreported. In the midst of what could be the largest whooping cough outbreak in more than 50 years — and the death of six infants under 3 months of age — California health officials are recommending booster shots for nearly everyone in the state, especially health care workers, parents, and anyone who may come in contact with babies. Whooping cough cases have been increasing since the 1980s, partly because of better diagnostic tests, according to the Centers for Disease Control and Prevention. It is incredibly contagious, sickening about 90 percent of people who are exposed to it. The state health department is providing whooping cough booster shots to new mothers and other close contacts of infants at all birthing

hospitals, community health centers and local health departments. Source: http://www.usatoday.com/news/health/2010-07-27-pertussis27_st_N.htm

TRANSPORTATION

Passenger rail systems vulnerable, GAO study says. Based on intelligence indicating that Al Qaeda and associated movements continue to express interest in attacking U.S. mass transit systems, the Government Accountability Office (GAO) has issued a redacted version of a classified report on "explosives detection technologies [that] are available or in development that could help secure passenger rail systems." However, GAO noted that "while these technologies show promise in certain environments, their potential limitations in the rail environment need to be considered and their use tailored to individual rail systems." In its report, Explosives Detection Technologies to Protect Passenger Rail, GAO did not make any specific recommendations, but it did raise "various policy considerations." The report pointed to the fact that the TSA and passenger rail operators share the responsibility for security, which is said could complicate decisions. In addition, the GAO recommended the use of risk-management principles to guide decision-making related to technology and resource allocation. Source: http://www.hstoday.us/content/view/14138/149/

Napolitano announces general aviation security measures. Despite a keen terrorist interest in the use of aircraft as missiles to strike targets, the Department of Homeland Security (DHS) has done little to date to secure general aviation fields, which house private jets and planes. DHS inched closer to strengthening general aviation security measures July 26, extending a transportation public awareness campaign to the airfields, and standardizing the vetting process for passengers and crew on general aviation aircraft. The DHS Secretary announced the extension of the campaign to general aviation while visiting the 2010 Experimental Aircraft Association (EAA) AirVenture air show in Oshkosh, Wisconsin, earlier this week. "This new component of 'If You See Something, Say Something' will enable general aviation passengers and crew to better recognize and report behaviors and indicators associated with new and evolving threats," the Secretary said in a statement. "We are also transitioning to a streamlined system for vetting travelers on general aviation flights to and from the United States to provide a single, electronic screening process while maintaining robust security standards." Congress and the U.S. President have voiced a renewed interest in general aviation security standards in recent months after a distraught software engineer flew a small private plane into a building housing IRS offices in Austin, Texas, in the spring, killing two people, including the pilot, and injuring 13 others. Source: http://www.examiner.com/x-59281-DC-Homeland-Security-Examiner~y2010m7d27-Napolitano-Announces-General-Aviation-Security-Measures

150,000 U.S. bridges are rated 'deficient'. About 25 percent of the U.S. bridges remain "structurally deficient" or "functionally obsolete"; the deterioration of bridges in the United States is the direct result of a confluence of three developments: the system is aging; the costs of maintaining bridges is high; and traffic on these bridges is steadily increasing. The number of deficient bridges has declined by nearly 12 percent since 1998, but about 150,000 bridges — nearly one in four — still are considered deficient, according to the latest data from the Federal Highway Administration (FHA). The overall drop can be attributed to improvements in local and rural bridges, according to the Government Accountability Office (GAO), but the number of deficient bridges in urban areas has increased 11 percent since 1998. A bridge termed structurally deficient or functionally obsolete may

not collapse tomorrow, but it is substandard. Source: http://homelandsecuritynewswire.com/150000-us-bridges-are-rated-deficient

(Illinois) **Flooding causes highway closure in Chicago area.** Flooding closed a major interstate in the Chicago area July 24, and caused heavy traffic delays on other roads. Interstate 290 closed between Mannheim Road and 25th Avenue, and standing water slowed traffic around Western Avenue. The Illinois Department of Transportation said at least eight cars have been reported under water. There was also standing water on Interstate 90/94 both north and south of the Loop. North of the Loop, standing water was reported around Addison Street, and south of the Loop, there was water between 83rd and 87th streets. Southbound traffic was being diverted at 83rd Street. Source: http://www.chicagotribune.com/news/chi-ap-il-chicagoflooding,0,4356596.story

Water and Dams

Invasive mussels pose threat to dams. The expected arrival of invasive mussels in the Columbia River Basin in Washington could cost $100 million a year to fight, according to a new report done for the Northwest Power and Conservation Council. The dime-sized freshwater mussels pose a threat to dams, irrigation systems and native fish species, said the report from a panel of economists. "While the mussels have not infested the Columbia River Basin yet, it may be just a matter of time," the council said in a statement, adding that efforts should still be made to stop or at least delay an invasion. The best deterrent is a combination of watercraft inspections, public information and continued scientific research, the report said. Eradicating the mussels is virtually impossible. They attach to almost anything and can clog drains and pipes, freeze up cooling systems, kill off native species and render power boats inoperable. In the Columbia River Basin, the new report estimated costs of cleaning water intakes and related equipment at federal hydropower dams on the Columbia and Snake rivers at $16 million a year, plus $5 million a year for other dams. Cleaning spillway gates, fish-bypass screens and related equipment would cost about $3 million to $10 million a year at the federal dams. Replacing filtration systems at 20 fish hatcheries would cost $1 million each. Cleaning recreation facilities, including water supplies, docks and boats, could run $50 million or more a year. Source: http://seattletimes.nwsource.com/html/localnews/2012475261_mussels29.html

(Iowa) **Experts worry about increase in deficient U.S. dams.** The failure of the 88-year-old dam at northeast Iowa's Lake Delhi comes when experts have been warning of potentially catastrophic consequences involving thousands of aging U.S. dams. The American Society of Civil Engineers, in a report on infrastructure last year, gave a "D" to the nation's system of 85,000 dams. The average dam is 51 years old, and more than 4,000 are deemed deficient, including some 1,800 that could potentially cause a loss of life if they failed. One of the worries is that new development is occurring below many dams, dramatically increasing the consequences of failure, the group said. Built in 1922, the Lake Delhi dam was considered structurally sound and met state standards for a moderate hazard dam, which meant that a loss of life was not expected downstream if the dam failed, said a dam safety engineer for the Iowa Department of Natural Resources. But improvements to the Lake Delhi dam could have averted Saturday's failure, he said. Those could have included construction of an emergency spillway or additional dam gates to accommodate a record flow of water without washing out the dam's earthen portion. If the Lake Delhi dam is rebuilt, an emergency spillway or additional gates will be required. Another alternative would be a design allowing floodwaters to safely flow over the structure. That could be done by "armoring" the back slope with rock or concrete so that flow

would not wash out the soil. A total of 31 Iowa dams are listed as deficient due to either hydraulic or structural problems, state officials said. None of the dams on the Iowa list are considered to be in a state of imminent failure. Source: http://www.desmoinesregister.com/article/20100727/NEWS10/7270358/-1/WATCHDOG/Experts-worry-about-increase-in-deficient-U.S.-dams

North Dakota Homeland Security Contacts

To report a homeland security incident, please contact your local law enforcement agency or one of these agencies: Fusion Center (24/7): 866-885-8295(IN ND ONLY); Email: ndslic@nd.gov ; Fax: **701-328-8175**
State Radio: 800-472-2121 Bureau of Criminal Investigation: 701-328-5500 Highway Patrol: 701-328-2455
US Attorney's Office Intel Analyst: 701-297-7400 Bismarck FBI: 701-223-4875 Fargo FBI: 701-232-7241

To contribute to this summary or if you have questions or comments, please contact:

Kirk Hagel, ND Division of Homeland Security kihagel@nd.gov, **701-328-8168**